John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

William B. Federman
OK Bar No. 2853
Kennedy M. Brian
OK Bar No. 34617
(*pro hac vice applications forthcoming*)
wbf@federmanlaw.com
kpb@federmanlaw.com
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Fax: (405) 239-2112

Attorneys for Plaintiff and the Proposed Class

THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

JOHN SJODIN, on behalf of himself and on behalf of all others similarly situated,

Plaintiff,

v.

CITY OF HOPE,

Defendant.

Case No. _____

CLASS ACTION

COMPLAINT FOR DAMAGES AND EQUITABLE RELIEF FOR:

1. **NEGLIGENCE**
2. **NEGLIGENCE PER SE**
3. **BREACH OF IMPLIED CONTRACT**
4. **COMMON LAW INVASION**

John Sjodin ("Plaintiff)" brings this Class Action Complaint against City of Hope ("Defendant"), on behalf of himself and all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII") and protected health information ("PHI") including, but not limited to, contact information (e.g., email address, phone number), date of birth, Social Security number, driver's license or other government identification, financial details (e.g., bank account and/or credit card details, health insurance information, medical records and information about medical history and/or associated conditions, and/or unique identifiers to associate individuals with City of Hope (e.g., medical record

number) (collectively, PII and PHI are referred to as "Private Information" or "Personal Information").[1]

2. Defendant states it is a world-renowned pioneer in cancer research, treatment and prevention and home to a National Cancer Institute (NCI)-designated comprehensive cancer center.[2]

3. To provide medical services, and in the ordinary course of Defendant's business, Defendant acquires, possesses, analyzes, and otherwise utilizes Plaintiff's and Class Members' Private Information.

4. As a non-profit corporation doing business in California and having employees and patients in California, Defendant is legally required to protect personal information from unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction.

5. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Plaintiff and hundreds of thousands of other similarly situated persons in a massive and preventable cyberattack.

6. Between September 19, 2023 and October 12, 2023, cybercriminals infiltrated Defendant's inadequately protected network servers and accessed and exfiltrated highly sensitive Private Information belonging to Plaintiff and Class Members which was being kept unprotected and unencrypted (the "Data Breach").[3]

7. Plaintiff further seeks to hold Defendant responsible for not ensuring it maintained the Private Information in a manner consistent with industry standards.

8. While Defendant claims to have discovered the Data Breach as early as October 13, 2023, Defendant did not begin informing victims of the Data Breach until December 14, 2023—two months later.[4] Indeed, Plaintiff and Class Members were wholly unaware of the Data Breach until they received Notice Letters from

[1] *See* Ex. 1 (Notice Letter).
[2] https://www.cityofhope.org/.
[3] https://www.cityofhope.org/notice-of-data-security-incident.
[4] *See* Ex. 1.

Defendant. During this time, Plaintiff and Class Members were unaware that their sensitive Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

9. The Notice Letter provides no further information regarding the Data Breach and only recommends how victims can place a fraud alert or credit freeze on their account and how to sign up for the limited, and abbreviated identity monitoring services Defendant offered to only certain Class Members in response to the Data Breach. The Notice Letter does not explain how the Data Breach occurred, what steps Defendant took following the Data Breach, whether Defendant made any changes to its data security, or most importantly, whether Plaintiff's and Class Members' Private Information remains in the possession of criminals.

10. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

11. By acquiring, utilizing, and benefiting from Plaintiff's and Class Members' Private Information for its business purposes, Defendant owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiff and Class Members. These duties required Defendant to design and implement adequate data security systems to protect Plaintiff's and Class Members' Private Information in its possession and to keep Plaintiff's and Class Members' Private Information confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

12. Defendant breached these duties by failing to implement adequate data security measures and protocols to properly safeguard and protect Plaintiff's and Class Members' Private Information from a foreseeable cyberattack on its systems that resulted in the unauthorized access and theft of Plaintiff's and Class Members' Private Information.

13. Currently, the full extent of the types of Private Information, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant, its agents, counsel, and forensic security vendors at this phase of the litigation.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, Plaintiff's and Class Members' Private Information was compromised through disclosure to an unknown and unauthorized criminal third party.

15. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

16. Based on the type of sophisticated and targeted criminal activity, the type of Private Information involved, and Defendant's admission that the Private Information was accessed, it can be concluded that the unauthorized criminal third

party was able to successfully target Plaintiff's and Class Members' Private Information, infiltrate and gain access to Defendant's network, and exfiltrate Plaintiff's and Class Members' Private Information, including full names, Social Security numbers, email addresses, dates of birth, driver's license numbers, and financial information, for the purposes of utilizing or selling the Private Information for use in future fraud and identity theft related cases.

17. As a result of Defendant's failures and the Data Breach, Plaintiff's and Class Members' identities are now at a current and substantial imminent and ongoing risk of identity theft and shall remain at risk for the rest of their lives.

18. As Defendant instructed, advised, and warned in its Notice Letter discussed below, Plaintiff and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

19. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time heeding Defendant' warnings and following its instructions in the Notice Letter; (g) deprivation of value of their Private Information; (h) invasions of their privacy; and (i) the continued risk to their Private Information, which remains in the possession of

Defendant, and which is subject to further breaches, so long as Defendant fail to undertake appropriate and adequate measures to protect it.

20. Plaintiff brings this action on behalf of all persons whose Private Information was compromised due to Defendant's failure to adequately protect Plaintiff's and Class Members' Private Information. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserts claims on behalf of the Class for negligence, negligence per se, unjust enrichment, breach of implied contract, declaratory judgment, and common law invasion of privacy. Plaintiff also brings claims on behalf of a California subclass for violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, the California Customer Records Act, Cal. Civ. Code § 1798.80 *et seq.*, and violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.*

PARTIES

21. Plaintiff **John Sjodin** is an adult individual and, at all relevant times herein, a resident and citizen of the state of California, residing in Upland, California.

22. Defendant **City of Hope** is a nonprofit corporation with its principal place of business located at 1500 E. Duarte Road, Duarte, California 91010.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, is a citizen of a state different from Defendant. Defendant is a citizen of the state of California and the plaintiff class and/or subclasses defined herein include citizens of other states, including California.

24. This Court has general personal jurisdiction over Defendant City of Hope because City of Hope is registered to do business in California with the

California Secretary of State. Defendant regularly contracts with a multitude of businesses, organizations and consumers in California to provide medical and health care related services. The Court has specific personal jurisdiction over City of Hope because the claims in this action stem from its specific contacts with the State of California — namely, Defendant's provision of medical and health care related services to a multitude of patients in California, Defendant's collection, maintenance, and processing of the personal data of Californians in connection with such services, including but not limited to Defendant's employees, Defendant's failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent Data Breach.

25. Venue is proper under 18 U.S.C § 1391(b)(1) (b)(1)-(2) and (c)(2) because a substantial part of the events or omissions giving rise to the claims alleged herein occurred within this judicial district, specifically City of Hope's provision of medical and health care related services in California and within Los Angeles County, Defendant collection, maintenance, and processing of the personal data of California citizens in connection with such services, City of Hope's failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent security breach of such data in July and August 2023 that resulted from City of Hope's failure. In addition, Plaintiff is informed and believes and thereon alleges that members of the class and subclass defined below reside in the Central District, and Defendant has its corporate headquarters within the Central District.

FACTUAL BACKGROUND

26. City of Hope is a cancer treatment and research organization with cancer centers in Georgia, California, Illinois, and Arizona.[5]

[5] https://www.cityofhope.org/.

27. City of Hope has over 30 clinical network locations, 11,000 employees, and services over 131,000 patients per year.[6]

28. City of Hope had approximately $335 million in revenue in 2022 and total assets of $2.5 billion.[7]

29. Upon information and belief, Defendant provides a HIPPA Notice to every patient upon request.

30. As a condition of providing medical care and/or medical billing, Defendant compiles, retains and stores its patients and employees' sensitive information including their names, contact information (e.g., email addresses, phone numbers), dates of birth, Social Security numbers, driver's license or other government identification, financial details (e.g., bank account number and/or credit card details), health insurance information, medical records and information about medical history and/or associated conditions, and/ or unique identifiers to associate individuals with City of Hope (e.g., medical record number).[8]

31. Defendant has served thousands of individuals since its founding and has created and maintains a massive repository of Personal Information, acting as a particularly lucrative target for data thieves looking to obtain, misuse, or sell patient data.

32. In the ordinary course of its business, Defendant maintains the Private Information of its patients, customers, current and past employees, and others including but not limited to full names, Social Security numbers, addresses, dates of birth, driver's license numbers, and financial information.

33. Additionally, City of Hope may receive Private Information from other individuals and/or organizations including Plaintiff's and Class Members'

[6] https://www.cityofhope.org/sites/www/files/2023-10/2022-Annual-Report.pdf.
[7] https://projects.propublica.org/nonprofits/organizations/953435919.
[8] *See* Ex. 1.

employers, insurance carriers, and in connection with enrollment in employee insurance and retirement benefit plans.

34. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to consumers, Defendant, upon information and belief, promises to, among other things: keep protected health information private; comply with healthcare industry standards related to data security and Private Information, inform consumers of its legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to medical care and treatment, and, provide adequate notice to individuals if their Private Information is disclosed without authorization.

35. As a HIPAA covered business entity (*see infra*), City of Hope is required to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured protected health information as in the case of the Data Breach complained of herein.

36. However, City of Hope did not maintain adequate security to protect its systems from infiltration by cybercriminals, and it waited nearly 2 months to disclose the Data Breach publicly.

37. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

38. At every step, Defendant stores Plaintiff's and Class Members' sensitive Private Information and has a duty to protect that Private Information from unauthorized access.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

40. Plaintiff and Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use their Private Information solely for proper business and healthcare related services and purposes, and to prevent the unauthorized disclosure of their Private Information.

City of Hope is a HIPAA Covered Entity

41. City of Hope is a HIPAA covered entity that provides healthcare and medical services. As a regular and necessary part of its business, City of Hope collects and custodies the highly sensitive Private Information of its patients and clients' patients.

42. City of Hope is required under federal and state law to maintain the strictest confidentiality of the patient's Private Information that it requires, receives, and collects, and City of Hope is further required to maintain sufficient safeguards to protect that Private Information from being accessed by unauthorized third parties.

43. As a HIPAA covered entity, City of Hope is required to ensure that it will implement adequate safeguards to prevent unauthorized use or disclosure of Private Information, including by implementing requirements of the HIPAA Security Rule and to report any unauthorized use or disclosure of Private Information, including incidents that constitute breaches of unsecured PHI as in the case of the Data Breach complained of herein.

44. Due to the nature of City of Hope's business, which includes providing a range of medical services, City of Hope would be unable to engage in its regular business activities without collecting and aggregating Private Information that it knows and understands to be sensitive and confidential.

45. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, City of Hope assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

46. Plaintiff and Class Members were current and former patients, customers, employees, and contractors whose Private Information was maintained by City of Hope, or who received health-related or other services from City of Hope, and directly or indirectly entrusted City of Hope with their Private Information.

47. Plaintiff and the Class Members relied on City of Hope to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information. Plaintiff and Class Members reasonably expected that City of Hope would safeguard and keep their Private Information confidential.

48. As described throughout this Complaint, City of Hope did not reasonably protect, secure, or store Plaintiff's and Class Members' Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures that it knew or should have known were insufficient to reasonably protect the highly sensitive information City of Hope maintained. Consequently, cybercriminals circumvented City of Hope's security measures, resulting in a significant and preventable data breach.

The Data Breach and Notice Letter

49. According to City of Hope, on or about October 13, 2023, City of Hope became aware of suspicious activity on a subset of its systems and immediately instituted mitigation measures to minimize any disruption to its operations.[9]

[9] *See* Ex. 1.

50. After an investigation, City of Hope determined that an unauthorized third party accessed a subset of its systems and obtained copies of some files between September 19, 2023, and October 12, 2023.[10]

51. The impacted personal information identified thus far varies by individual but may have included name, contact information (e.g., email address, phone number), date of birth, social security number, driver's license or other government identification, financial details (e.g., bank account number and/or credit card details), health insurance information, medical records and information about medical history and/or associated conditions, and/ or unique identifiers to associate individuals with City of Hope (e.g., medical record number).[11]

52. The investigation determined that the accessed systems contained Private Information belonging to Plaintiff and Class Members. Upon information and belief, this Private Information was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor. In other words, Plaintiff's and Class Members' Private Information was exfiltrated and stolen in the attack.

53. While City of Hope stated in the Notice Letter that the Data Breach occurred between September 19, 2023, and October 12, 2023, City of Hope did not begin notifying victims until December 2023.[12]

54. Defendant had obligations created by contract, industry standards, HIPPA, common law, and its own promises and representations to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

55. Plaintiff and Class Members provided their Private Information directly, or indirectly, to Defendant with the reasonable expectation and mutual understanding

[10] *Id.*
[11] *Id.*
[12] *Id.*

that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

56. Through its Notice Letter, City of Hope recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to take steps to mitigate their risk of identity theft, such as reviewing financial accounts, and reviewing credit reports for possible fraud.[13]

57. City of Hope has offered abbreviated, non-automatic credit monitoring services to victims thereby identifying the harm posed to Plaintiff and Class Members as a result of the Data Breach, which does not adequately address the lifelong harm that victims face following the Data Breach. Indeed, the Data Breach involves Private Information that cannot be changed, such as Social Security numbers.

58. Beginning on or around December 14, 2023, Defendant began issuing Notice Letters to Plaintiff and Class Members.[14]

59. Defendant issued another round of Notice Letters in or around April 2, 2024. [15]

60. In total, Defendant claims 827,149 were impacted by the Data Breach.[16]

61. The Notice Letters sent to Plaintiff and Class Members stated sensitive information including names, contact information (e.g., email addresses, phone numbers), dates of birth, social security numbers, driver's license or other government identification, financial details (e.g., bank account number and/or credit card details), health insurance information, medical records and information about medical history and/or associated conditions, and/ or unique identifiers to associate

[13] *Id.*
[14] https://apps.web.maine.gov/online/aeviewer/ME/40/1bb296e2-ea79-438c-b357-28ef738a0bf6.shtml.
[15] *Id.*
[16] *Id.*

individuals with City of Hope (e.g., medical record number) was accessed and obtained in the Data Breach.[17]

62. As a result of the Data Breach, Plaintiff and hundreds of thousands of Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

63. Defendant waited approximately two months to disclose the Data Brach to Plaintiff and Class Members. As a result of this delay, Plaintiff and Class Members had no idea their Private Information had been compromised in the Data Breach, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

64. Defendant's failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Private Information.

65. This Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiff and Class Members.

66. As a HIPAA covered entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which City of Hope was aware and knew it had a duty to guard against. It is well-known that healthcare businesses such as Defendant, which collect and store the confidential and sensitive PII/PHI of thousands of individuals, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the

[17] *Id.*

implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training.

67. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiff and Class Members.

68. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect its patients' Private Information or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' and consumers' Private Information.

69. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their Private Information which includes information that is static, does not change, and can be used to commit myriad financial crimes.

70. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use their Private Information for authorized purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand Defendant safeguard their Private Information.

71. The unencrypted Private Information of Plaintiff and Class Members will likely be offered for sale on the dark web as is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. In turn, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

72. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were

maintaining for Plaintiff and Class Members, causing the exposure of Private Information.

73. Due to City of Hope's inadequate security measures and its delayed notice to victims, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

The Data Breach Was Foreseeable

74. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry and other industries holding significant amounts of PII and PHI preceding the date of the breach.

75. At all relevant times, City of Hope knew, or should have known, that Plaintiff, and Class Members' Private Information was a target for malicious actors. Despite such knowledge, City of Hope failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' Private Information from cyberattacks that City of Hope should have anticipated and guarded against.

76. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, like Plaintiff and Class Members.

77. In light of recent high profile data breaches at other health care providers, Defendant knew or should have known that their electronic records and consumers' Private Information would be targeted by cybercriminals and ransomware attack groups.

78. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2022 report, the healthcare compliance company Protenus found that there were 905 medical data breaches in 2021, leaving over 50 million

patient records exposed for 700 of the 2021 incidents. This is an increase from the 758 medical data breaches that Protenus compiled in 2020.[18]

79. The healthcare sector suffered about 337 breaches in the first half of 2022 alone, according to Fortified Health Security's mid-year report released in July. The percentage of healthcare breaches attributed to malicious activity rose more than five percentage points in the first six months of 2022 to account for nearly 80 percent of all reported incidents.[19]

80. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

81. Indeed, cyberattacks against the healthcare industry have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[20]

---

[18] *2022 Breach Barometer*, PROTENUS, *see* https://blog.protenus.com/key-takeaways-from- the-2022-breach-barometer.

[19] Jill McKeon, *Health Sector Suffered 337 Healthcare Data Breaches in First Half of Year*, Cybersecurity News (July 19, 2022), available at: https://healthitsecurity.com/news/health-sector- suffered-337-healthcare-data-breaches-in-first-half-of-year.

[20] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011),

82. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[21] A cybercriminal who steals a person's PHI can end up with as many as "seven to 10 personal identifying characteristics of an individual."[22] A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident in 2010, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[23]

83. Cyberattacks on healthcare entities like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[24]

84. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the

---

https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

[21] *See* Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH MAGAZINE (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare- data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").

[22] *Id.*

[23] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/.

[24] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents." [25]

85. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[26]

86. Patient records, like those stolen from City of Hope, are "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[27]

87. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

88. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[28]

89. City of Hope was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has

---

[25] https://www.hipaajournal.com/why-do-criminals-target-medical-records.
[26] *See id.*
[27] *See id*.
[28] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[29]

90. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[30]

91. As implied by the above AMA quote, stolen Private Information can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff and Class Members.

92. The U.S. Department of Health and Human Services and the Office of Consumer Rights urges the use of encryption of data containing sensitive personal information. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, formerly OCR's deputy director of health information privacy, stated in 2014 that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[31]

---

[29] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820.

[30] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED.ASS'N (Oct 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

[31] https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen-

93. As a HIPAA covered entity, City of Hope should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the Private Information stored in its unprotected files.

Defendant Fails to Comply with FTC Guidelines

94. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

95. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[32] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[33]

96. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

---

laptops.

[32] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[33] *Id*.

97. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

98. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

99. Defendant failed to properly implement basic data security practices.

100. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

101. Defendant was at all times fully aware of its obligation to protect the Private Information of customers and patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

City of Hope Fails to Comply with Industry Standards

102. As shown above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

103. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a

key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

104. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

105. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

106. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

City of Hope's Conduct Violates HIPAA Obligations to Safeguard Private Information

107. As a medical services provider, City of Hope is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

108. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

109. City of Hope is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[5] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

110. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information that is kept or transferred in electronic form.

111. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

112. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

113. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

114. The Data Breach resulted from a combination of insufficiencies that demonstrate City of Hope failed to comply with safeguards mandated by HIPAA regulations.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

115. Cyberattacks and data breaches at healthcare companies and partner companies like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

116. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[34]

117. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[35]

118. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[36]

119. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial

[34] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[35] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203.

[36] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

120. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[37]

121. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

122. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal

[37] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps.

information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

123. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[38]

124. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

125. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

126. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

127. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

128. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market,

[38] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

129. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

130. Private Information can sell for as much as $363 per record according to the Infosec Institute.[39] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

131. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[40] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[41] Each of these fraudulent activities is difficult to detect. An individual may not know that his or his Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

132. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

133. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social

---

[39] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[40] *Identity Theft and Your Social Security Number*, Social Security Administration (2018). Available at https://www.ssa.gov/pubs/EN-05-10064.pdf.

[41] *Id*.

Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[42]

134. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[43]

135. Medical information is especially valuable to identity thieves.

136. Theft of PHI, in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[44]

137. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

138. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a

---

[42] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[43] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[44] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft.

Facebook account.[45] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[46]

139. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

140. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was on notice of the substantial and foreseeable risk of harm from a data breach, yet City of Hope failed to properly prepare for that risk.

141. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant'sunlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' and customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

---

[45] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong.

[46] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

p. Failing to adhere to industry standards for cybersecurity as discussed above; and

q. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

142. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access City of Hope' computer network and systems which contained unsecured and unencrypted Private Information.

143. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

Defendant's Response to the Data Breach is Inadequate to Protect Plaintiff and the Class

144. Defendant failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

145. Defendant stated that the Data Breach occurred between September 19, 2023, and October 12, 2023. However, Defendant did not start notifying affected individuals until at least December 2023. Even then, Defendant provided only vague information. As a result, Plaintiff and Class Members are unsure as to the scope of information that was compromised and the risks they face.

146. Defendant's failure to timely notify the victims of its Data Breach meant that Plaintiff and Class Members were unable to take affirmative measures to prevent or mitigate the resulting harm.

Plaintiff's and Class Members' Damages

147. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiff and Class Members have all suffered damages and will face a substantial risk of additional injuries for the rest of their lives. Yet, to date, Defendant has merely offered to provide certain victims of the Data Breach with limited, abbreviated subscriptions to identity monitoring services. This does nothing to compensate Plaintiff or Class Members for many of the injuries they have already suffered. Nor will it prevent additional harm from befalling Plaintiff and Class Members as a result of the Data Breach. And at the conclusion of these limited subscriptions, victims will be required to pay for such services out of their own pocket.

148. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

149. Plaintiff's and Class Members' Private Information were all compromised in the Data Breach and are now in the hands of the cybercriminals who accessed Defendant's computer system.

150. Since being notified of the Data Breach, Plaintiff Sjodin has spent time dealing with the impact of the Data Breach, valuable time Plaintiff Sjodin otherwise would have spent on other activities, including but not limited to work and/or recreation.

151. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring his accounts for fraudulent activity.

152. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

153. As a direct and proximate result of Defendant' conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

154. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

155. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

156. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

157. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

158. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

159. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of City of Hope' computer system(s) and Plaintiff's and Class Members' Private

Information. Thus, Plaintiff and the Class Members did not get what they paid for and agreed to.

160. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their medical accounts and sensitive information for misuse.

161. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for the rest of their lives.

162. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

163. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

164. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

Plaintiff Sjodin's Individual Experience

165. At the time of the Data Breach, Defendant retained Plaintiff Sjodin's Private Information in its system.

166. Plaintiff Sjodin was sent a Notice Letter dated April 2, 2024, informing him that Defendant experienced a Data Breach and that Plaintiff's Private Information, including his name, contact information (e.g., email address, phone number), date of birth, social security number, driver's license or other government identification, financial details (e.g., bank account number and/or credit card details), health insurance information, medical records and information about medical history and/or associated conditions, and/ or unique identifiers to associate individuals with City of Hope (e.g., medical record number) were compromised in the Data Breach.[47]

167. As a result of the Data Breach, Plaintiff Sjodin already spent **eleven (11) hours** dealing with the consequences of the Data Breach, which includes verifying the legitimacy of the Notice of Data Breach, researching credit monitoring and identity theft protection services, enrolling in credit monitoring services, and self-monitoring his accounts and/or credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. He has also spent a significant amount of time dealing with spam communications he has begun to

[47] *See* Ex. 1.

receive as a result of the Data Breach. This time was spent at Defendant's direction by way of the Notice Letter where Defendant advised Plaintiff Sjodin to remain vigilant for incidents of identity theft, and to mitigate his damages by, among other things, monitoring his accounts for fraudulent activity.

168. Plaintiff Sjodin is a cautious person and is therefore very careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Sjodin stores any documents containing his Private Information in a safe and secure location or destroys the documents.

169. The Data Breach caused Plaintiff Sjodin to suffer a loss of privacy.

170. The Data Breach has caused Plaintiff Sjodin to suffer imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of criminals and likely exploited on the Dark Web.

171. The loss of privacy and substantial present risk of imminent harm have caused Plaintiff Sjodin to suffer stress, fear, and anxiety as Plaintiff Sjodin is very concerned that his sensitive Private Information is now in the hands of data thieves and shall remain that way for the remainder of his lifetime and there is nothing Plaintiff Sjodin can do to retrieve his stolen Private Information from the cybercriminals.

172. Given the time Plaintiff Sjodin has lost investigating this data breach, taking steps to understand its full scope, determining the appropriate remedial steps, contacting counsel, etc., coupled with Plaintiff Sjodin's resultant and naturally foreseeable fears/concerns for the use of Plaintiff Sjodin's valuable Private Information, the damages articulated more specifically above are far from the full extent of the harm thereto.

CLASS ACTION ALLEGATIONS

173. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all other similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

174. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **Nationwide Class**: All persons in the United States whose PII and/or PHI was compromised in or as a result of Defendant's Data Breach that occurred on or around September 19, 2023 through October 12, 2023.

175. In addition, Plaintiff Sjodin also seeks to represent the following Subclass:

> **California Subclass:** All persons residing in California whose PII and/or PHI was compromised in or as a result of Defendant's Data Breach that occurred on or around September 19, 2023 through October 12, 2023.

176. The Nationwide Class, together with the Subclass, are collectively referred to herein as the "Classes" or the "Class."

177. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

178. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

179. This action has been brought and may be maintained as a class action under Rule 23 because there is a well-defined community of interest in the litigation and the proposed classes are ascertainable, as described further below:

a. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are at least 800,000 who were impacted by the Data Breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

b. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

i. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

ii. Whether Defendant had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

iii. Whether Defendant had duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

iv. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

v. Whether and when Defendant actually learned of the Data Breach;

vi. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

vii. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

viii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

ix. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

x. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

xi. Whether Defendant violated the consumer protection statutes invoked herein;

xii. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

xiii. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

xiv. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

c. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

d. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff

has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

e. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

180. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

181. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

182. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

183. Adequate notice can be given to Class Members directly using information maintained in Defendant's records. Among other means, potential notice to class members of this class action can be accomplished via United States mail to all individuals who received a copy of the September 29, 2023, data breach notice letter and/or through electronic mail and/or through publication.

184. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

185. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

186. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I

Negligence

(On Behalf of Plaintiff and the Nationwide Class)

187. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 186.

188. Plaintiff and the Class entrusted Defendant with their Private Information.

189. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

190. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

191. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

192. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

193. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain.

194. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Class.

195. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant, either directly or indirectly, with their confidential Private Information, a necessary part of obtaining services from Defendant.

196. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

197. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

198. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

199. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the Private Information of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

200. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

201. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

202. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

203. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiff and the Class.

204. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

205. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and the Class during the time the Private Information was within Defendant's possession or control.

206. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

207. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiff and the Class in the face of increased risk of theft.

208. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

209. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove Private Information it was no longer required to retain pursuant to regulations.

210. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

211. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the Private Information of Plaintiff and the Class would not have been compromised.

212. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

213. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and consumers and patients, which is recognized by laws and regulations including but not limited to HIPAA, the FTC Act, and common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

214. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at

issue in this case constitutes "protected health information" within the meaning of HIPAA.

215. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

216. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

217. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

218. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

219. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

220. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost

opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

221. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

222. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

223. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
Negligence *Per Se*
(On behalf of Plaintiff and the Nationwide Class)

224. Plaintiff realleges and incorporates by reference the paragraphs 1 through 186 as if fully set forth herein.

225. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as Defendant. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based on the FTC Act that also created a duty.

226. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as Defendant. Various FTC publications and data security breach orders further form the basis of Defendant's duty. In addition, individual states have enacted statutes based on the FTC Act that also created a duty.

227. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect personal information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of personal information it obtained and stored and the foreseeable consequences of a data breach.

228. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

229. Plaintiff and class members are consumers within the class of persons Section 5 of the FTC Act was meant to protect.

230. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the class.

231. As a direct and proximate result of Defendant's negligence, Plaintiff and class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT III
Breach Of Implied Contract
(On behalf of Plaintiff and the Nationwide Class)

232. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 186.

233. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

234. Plaintiff and the Class were required to and delivered their Private Information to Defendant as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

235. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of DefendantCity of Hope Holdings, Inc.regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

236. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services or Plaintiff and Class Members.

237. In accepting such information and payment for services, Plaintiff and the other Class Members entered into an implied contract with Defendant whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

238. In delivering their Private Information to Defendant and providing paying for healthcare services, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard the data as part of that service.

239. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

240. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

241. Plaintiff and the Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

242. Had Defendant disclosed to Plaintiff and the Class that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff

and the other Class Members would not have provided their Sensitive Information to Defendant.

243. Defendant recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

244. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Defendant.

245. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

246. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV
Invasion of Privacy
Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On behalf of Plaintiff and the Nationwide Class)

247. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 186.

248. To assert claims for intrusion upon seclusion, one must plead (1) that the defendant intentionally intruded into a matter as to which plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

249. Defendant intentionally intruded upon the solitude, seclusion and private affairs of Plaintiff and Class Members by intentionally configuring their systems in such a way that left them vulnerable to malware/ransomware attack, thus permitting unauthorized access to their systems, which compromised Plaintiff's and Class Members' personal information. Only Defendant had control over its systems.

250. Defendant's conduct is especially egregious and offensive as they failed to have adequate security measures in place to prevent, track, or detect in a timely fashion unauthorized access to Plaintiff's and Class Members' personal information.

251. At all times, Defendant was aware that Plaintiff's and Class Members' personal information in their possession contained highly sensitive and confidential personal information.

252. Plaintiff and Class Members have a reasonable expectation of privacy in their personal information, which also contains highly sensitive medical information.

253. Defendant intentionally configured their systems in such a way that stored Plaintiff's and Class Members' personal information to be left vulnerable to malware/ransomware attack without regard for Plaintiff's and Class Members' privacy interests.

254. The disclosure of the sensitive and confidential personal information of thousands of consumers, was highly offensive to Plaintiff and class members because it violated expectations of privacy that have been established by general social norms, including by granting access to information and data that is private and would not otherwise be disclosed.

255. Defendant's conduct would be highly offensive to a reasonable person in that it violated statutory and regulatory protections designed to protect highly sensitive information, in addition to social norms. Defendant's conduct would be especially egregious to a reasonable person as Defendant publicly disclosed Plaintiff's and Class Members' sensitive and confidential personal information without their consent, to an "unauthorized person," i.e., hackers.

256. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

257. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's intrusion upon seclusion and are entitled to just compensation.

258. Plaintiff and class members are entitled to appropriate relief, including compensatory damages for the harm to their privacy, loss of valuable rights and protections, and heightened stress, fear, anxiety, and risk of future invasions of privacy.

COUNT V

Violation of the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.*
(By Plaintiff and the California Class)

259. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 186.

260. In Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

261. Defendant is a "contractor" within the meaning of Civil Code § 56.05(d) within the meaning of Civil Code § 56.06 and/or a "business organized for the purpose of maintaining medical information" and/or a "business that offers software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of Defendant, within the meaning of Civil Code § 56.05(k).

262. Plaintiff and California subclass members are "patients" within the meaning of Civil Code § 56.05(k) and are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiff and California subclass members fear that disclosure of their medical information could subject them to harassment or abuse.

263. Plaintiff and California subclass members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant's computer network at the time of the unauthorized disclosure.

264. Defendant, through inadequate security, allowed unauthorized third-party access to Plaintiff's and California subclass members' medical information, without the prior written authorization of Plaintiff and California subclass members, as required by Civil Code § 56.10 of the CMIA.

265. In violation of Civil Code § 56.10(a), Defendant disclosed Plaintiff's and California subclass members' medical information without first obtaining an authorization. Plaintiff's and California subclass members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.10(a).

266. In violation of Civil Code § 56.10(e), Defendant further disclosed Plaintiff's and California subclass members' medical information to persons or entities not engaged in providing direct health care services to Plaintiff or California subclass members, or to their providers of health care or health care service plans or their insurers or self-insured employers.

267. Defendant violated Civil Code § 56.101 of the CMIA through its willful and knowing failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the California subclass members. Defendant's conduct with respect to the disclosure of confidential PII and PHI was willful and knowing because Defendant designed and implemented the computer network and security practices that gave rise to the unlawful disclosure.

268. In violation of Civil Code § 56.101(a), Defendant created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and class members' medical information in a manner that failed to preserve and breached the confidentiality of the information contained therein. Plaintiff's and California

subclass member' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a). 380. In violation of Civil Code § 56.101(a), Defendant negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiff's and California subclass members' medical information. Plaintiff's and California subclass members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(a).

269. Plaintiff's and California subclass members' medical information that was the subject of the unauthorized disclosure included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

270. In violation of Civil Code § 56.101(b)(1)(A), Defendant's electronic health record system or electronic medical record system failed to protect and preserve the integrity of electronic medical information. Plaintiff's and California subclass members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendant's violation of Civil Code § 56.101(b)(1)(A).

271. Defendant violated Civil Code § 56.36 of the CMIA through its failure to maintain and preserve the confidentiality of the medical information of Plaintiff and the California subclass members.

272. As a result of Defendant's above-described conduct, Plaintiff and California subclass members have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36. 385. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the unauthorized disclosure, and violation of the CMIA, Plaintiff and California subclass members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the

form of, *inter alia*, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud-risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII and PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII and PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

273. Plaintiff, individually and for each member of the Class, seeks nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiff and each California subclass member, and attorneys' fees, litigation expenses and court costs, pursuant to Civil Code § 56.35.

COUNT VI
Violation of the California Customer Records Act,
Cal. Civ. Code §§ 1798.80 *et seq.*,
(By Plaintiff and the California Subclass)

274. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 186.

275. Cal. Civ. Code § 1798.81.5 provides that "[i]t is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

276. Section 1798.81.5(b) further states that: "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to

the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

277. Cal. Civ. Code § 1798.84(b) provides that [a]ny customer injured by a violation of this title may institute a civil action to recover damages." Section 1798.84(e) further provides that "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

278. Plaintiff and members of the California subclass are "customers" within the meaning of Civ. Code § 1798.80(c) and 1798.84(b) because they are individuals who provided personal information to Defendant, directly and/or indirectly, for the purpose of obtaining a service from Defendant.

279. The personal information of Plaintiff and the California subclass at issue in this lawsuit constitutes "personal information" under § 1798.81.5(d)(1) in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

280. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the California subclass's personal information and that the risk of a data breach or theft was highly likely.

Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the California subclass. Specifically, Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information of Plaintiff and the California subclass from unauthorized access, destruction, use, modification, or disclosure. Defendant further subjected Plaintiff's and the California subclass's nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

281. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access, destruction, use, modification, or disclosure of the personal information of Plaintiff and the California subclass included hackers' access to, removal, deletion, destruction, use, modification, disabling, disclosure and/or conversion of the personal information of Plaintiff and the California subclass by the ransomware attackers and/or additional unauthorized third parties to whom those cybercriminals sold and/or otherwise transmitted the information.

282. As a direct and proximate result of Defendant's acts or omissions, Plaintiff and the California subclass were injured and lost money or property including, but not limited to, the loss of Plaintiff's and the subclass's legally protected interest in the confidentiality and privacy of their personal information, nominal damages, and additional losses described above. Plaintiff seeks compensatory damages as well as injunctive relief pursuant to Cal. Civ. Code § 1798.84(b).

283. Moreover, the California Customer Records Act further provides: "A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately

following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82.

284. Any person or business that is required to issue a security breach notification under the CRA must meet the following requirements under §1798.82(d):

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

i. the date of the breach,

ii. the estimated date of the breach, or

iii. the date range within which the breach occurred. The notification shall also include the date of the notice;

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided;

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number;

g. If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or

may have been breached if the breach exposed or may have exposed personal information.

285. Defendant failed to provide the legally compliant notice under § 1798.82(d) to Plaintiff and members of the California subclass. On information and belief, to date, Defendant has not sent written notice of the data breach to all impacted individuals. As a result, Defendant has violated § 1798.82 by not providing legally compliant and timely notice to all class members. Because not all members of the class have been notified of the breach, members could have taken action to protect their personal information but were unable to do so because they were not timely notified of the breach.

286. According to information and belief, many class members affected by the breach, have not received any notice at all from Defendant in violation of Section 1798.82(d).

287. As a result of the violations of Cal. Civ. Code § 1798.82, Plaintiff and class members suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

288. As a direct consequence of the actions as identified above, Plaintiff and class members incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, increased stress, fear, and anxiety, harm to their constitutional right to privacy, lost time dedicated to the investigation of the breach and effort to cure any resulting harm, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal, financial, and payroll information disclosed, that they would not have otherwise incurred, and are entitled to recover compensatory damages according to proof pursuant to § 1798.84(b).

COUNT VII
Violation of the California Unfair Competition Law
Cal. Civ. Code §§ 17200 *et seq.*,
(By Plaintiff and the California Subclass)

289. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 186.

290. Defendant is a "person" defined by Cal. Bus. & Prof. Code § 17201.

291. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by engaging in unlawful and unfair business acts and practices.

292. Defendant' "unfair" acts and practices include:

293. Defendant failed to implement and maintain reasonable security measures to protect Plaintiff's and California subclass members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Defendant data breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

294. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56);

295. Defendant's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused; and

296. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

297. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, and California common law.

298. Defendant's unlawful and unfair practices include:

299. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California subclass members' personal information, which was a direct and proximate cause of the Defendant data breach;

300. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Defendant data breach;

301. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, and California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56), which was a direct and proximate cause of the Defendant data breach;

302. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California subclass members' personal information, including by implementing and maintaining reasonable security measures;

303. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C.

§ 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56);

304. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California subclass members' personal information; and

305. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Confidentiality of Medical Information Act (Cal. Civ. Code § 56).

306. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal information.

307. As a direct and proximate result of Defendant's unfair and unlawful acts and practices, Plaintiff and California subclass members were injured and lost money or property, which would not have occurred but for the unfair and unlawful acts alleged herein, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

308. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

309. Plaintiff and class members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

310. By deceptively storing, collecting, and disclosing their personal information, Defendant has taken money or property from Plaintiff and California subclass members.

311. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California subclass members' rights. Past data breaches put Defendant on notice that its security and privacy protections were inadequate.

312. Plaintiff and California subclass members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair and unlawful business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT VIII
DECLARATORY JUDGMENT
(By Plaintiff and the Nationwide Class)

313. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 186.

314. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

315. As previously alleged, Plaintiff and members of the Class entered into implied contracts with Defendant, which contracts required Defendant to provide adequate security for the Private Information collected from Plaintiff and the Class.

316. Defendant owed and still owes a duty of care to Plaintiff and Class members that require it to adequately secure Plaintiff's and Class members' Private Information.

317. Upon reason and belief, Defendant still possesses the Private Information of Plaintiff and the Class members.

318. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class members.

319. Since the Data Breach, Defendant has not yet announced any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breaches to occur and go undetected and, thereby, prevent further attacks.

320. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the Private Information in Defendant's possession is even more vulnerable to cyberattack.

321. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

322. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

323. Plaintiff and the Class, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment employee data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;

f. Ordering that Defendant conduct regular database scanning and security checks; and

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

COUNT IX
UNJUST ENRICHMENT
(By Plaintiff and the Nationwide Class)

324. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 186.

325. This claim is pleaded in the alternative to the breach implied contract claim above.

326. Plaintiff and Class Members conferred a monetary benefit to Defendant by paying Defendant for medical services.

327. Defendant knew that Plaintiffs and Class Members conferred a monetary benefit to Defendant when they accepted and retained that benefit.

328. Defendant was supposed to use some of the monetary benefit provided to them from Plaintiff and Class members to secure the Private Information belonging to Plaintiff and Class members by paying for costs of adequate data management and security.

329. Defendant should not be permitted to retain any monetary benefit as a result of its failure to implement necessary security measures to protect the Private Information of Plaintiff and Class members.

330. Defendant gained access to the Plaintiff's and Class members' Private Information through inequitable means because Defendant failed to disclose that it used inadequate security measures.

331. Plaintiff and Class members were unaware of the inadequate security measures and would not have provided their Private Information to Defendant had they known of the inadequate security measures.

332. To the extent that this cause of action is pled in the alternative to the others, Plaintiff and Class members have no adequate remedy at law.

333. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate

measures to protect the Private Information of Plaintiff and Class members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class members.

334. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

335. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds from the monetary benefit that it unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Classes, and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's

network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Private Information, as well as protecting the Private Information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their

confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages in an amount to be proven at trial, in excess of $5,000,000.

E. Statutory damages pursuant to Cal. Civ. Code § 56.36(b);

F. Reasonable attorneys' fees, including pursuant to Cal. Civ. Pro. Code § 1021.5;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the Nationwide Class and California subclass, hereby demands that this matter be tried before a jury.

Date: April 22, 2024

Respectfully Submitted,

/s/ John J. Nelson

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

William B. Federman
OK Bar No. 2853
Kennedy M. Brian
OK Bar No. 34617
(*pro hac vice applications forthcoming*)
wbf@federmanlaw.com
kpb@federmanlaw.com
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Fax: (405) 239-2112

Counsel for Plaintiff and Putative Class